I. Введение

Фишинговые атаки в Великобритании находятся на подъёме, киберпреступники используют все более изощренные методы для обмана отдельных лиц и организаций с целью получения конфиденциальной информации. Национальный центр кибербезопасности (NCSC) и другие организации, активно работают над борьбой с этими угрозами, предоставляя отдельным лицам ресурсы для сообщений о подозрительных действиях и предлагая рекомендации о том, как не стать жертвой. По данным за 2023 год 74% нарушений связаны с человеческим фактором, который включает атаки социальной инженерии, ошибки или неправильное использование.

Новый вид мошенничества включают QR-фишинг, при котором преступники скрывают вредоносные ссылки в QR-кодах и размещают их в социальных сетях в рамках активностей для фанатов, поиска билетов и т.п..

Искусственный интеллект (ИИ) также используется киберпреступниками для усиления своих фишинговых атак. С его помощью создаются убедительные персонализированные фишинговые электронные письма, и дипфейки, используемых для имитации биометрической аутентификации с использованием лиц и голоса

II. Борьба с фишингом в Великобритании

Борьба с фишингом в Великобритании предполагает комплексный подход, который включает правительственные инициативы, сотрудничество с технологическими компаниями, действия правоохранительных органов, а также образовательные программы.

Правительство Великобритании предприняло несколько шагов по борьбе с фишингом и другими формами киберпреступности. Национальный центр кибербезопасности (NCSC), организация правительства Великобритании, имеет полномочия расследовать и удалять мошеннические адреса электронной почты и веб-сайты. Правительство подписало соглашение с некоторыми крупнейшими технологическими компаниями, которая обязывает блокировать и удалять мошеннический контент со своих платформ. Также правительство запустило новую стратегию борьбы с мошенничеством, в которую входит Национальное подразделение по борьбе с мошенничеством, возглавляемое Национальным агентством по борьбе с преступностью и полицией Лондон-Сити. Национальное агентство по борьбе с преступностью (NCA) стремится повысить устойчивость Великобритании к кибератакам и улучшить реакцию правоохранительных органов на угрозу киберпреступности.

Повышение образования и осведомлённости рассматривается как ключ к предотвращению фишинговых атак. Различные организации предлагают учебные курсы по повышению осведомлённости о фишинге, которые обучают отдельных лиц и сотрудников тому, как распознавать такие атаки и предотвращать их. NCSC предоставляет рекомендации по защите от фишинговых атак, а также по выявлению мошеннических электронных писем, текстовых сообщений, веб-сайтов и звонков и сообщению о них.

Сотрудничество с международными партнёрами также имеет решающее значение в борьбе с фишингом, особенно учитывая, что многие киберугрозы исходят из-за рубежа. NCSC Великобритании объединила усилия с Агентством национальной безопасности (АНБ) США и другими международными партнёрами, чтобы публиковать обновления о текущих угрозах и предоставлять рекомендации по защите от них.

III. Важность последствий фишинга

Фишинг в Великобритании представляет собой значительную и растущую угрозу для частных лиц, предприятий и критически важной инфраструктуры страны. Фишинговые атаки, которые часто включают обман людей с целью получения конфиденциальной информации или установки вредоносного ПО, становятся все более изощрёнными и распространёнными. Национальный центр кибербезопасности (NCSC) предупредил о целенаправленных фишинговых кампаниях против организаций и частных лиц Великобритании, подчеркнув сохраняющуюся и значительную угрозу критически важной инфраструктуре страны.

Финансовые последствия фишинга существенны, компании сообщают о больших убытках (…лишь бы не платить). Например, в 2021 году фишинговые атаки привели к убыткам на общую сумму 44,2 миллиона долларов по всему миру, а средние затраты организации на восстановление после утечки данных в Великобритании превышают 3,4 миллиона фунтов стерлингов.

Фишинг также оказывает значительное влияние на общественность. Примерно девять из десяти пользователей Интернета в Великобритании сталкивались с контентом, который, как они подозревали, является мошенничеством.

Кроме того, фишинг подрывает безопасность информационных систем и может привести к утечке данных, краже личных данных и финансовому мошенничеству. Использование уязвимости «человека» делает его критически важным для стратегий кибербезопасности.

A. Недавние фишинговые атаки в Великобритании

Фишинговые атаки остаются серьёзной угрозой кибербезопасности в Великобритании, и различные недавние примеры демонстрируют разнообразие тактик, используемых киберпреступниками.

- **Вишинг-атаки**: В ноябре 2023 года международная операция сорвала фишинговую кампанию, в результате которой жертвы были обмануты на десятки миллионов евро. Преступники осуществляли вишинговые (голосовой фишинг) атаки из колл-центров Украины и Чехии, выдавая себя за банковских служащих с целью перевода (вымогательства) денег
- **Фишинговая кампания для сотрудников отелей**: В том же месяце фишинговые кампании были нацелены на сотрудников отелей. Злоумышленники отправляли электронные письма сотрудникам, обманом заставляя их переходить по ссылке, по которой загружалась вредоносная infostealer-программа. После заражения злоумышленники удаляли данные клиентов
- **Поддельные электронные письма USPS**: В мае 2023 года USPS и Служба почтовой инспекции сообщили о распространении поддельных электронных писем, якобы, от должностных лиц USPS. В этих электронных письмах получателям предлагалось подтвердить свои личные данные о доставке, нажав кнопку, которая при открытии могла активировать вирус и украсть информацию
- **Фишинговая атака транспортного бизнеса Великобритании**: В первом квартале 2021 года транспортное предприятие Великобритании подверглось кибератаке, в результате которой сотрудникам организации было отправлено электронное письмо с документом, содержащим ссылку на поддельный портал. Поддельный портал требовал от получателя входа в систему с использованием учётных данных для проверки подлинности Office 365 / G-Suite. Когда получатели входили в систему, их учётные данные и парольные фразы собирались и затем использовались для доступа к почтовым ящикам жертв
- **QR-фишинг**: В 2024 году появилась новая форма фишинга под названием "квишинг", при которой преступники скрывают вредоносные ссылки в QR-кодах чтобы украсть личную информацию или загрузить вредоносное ПО. Этот тип фишинга может проявляться в виде электронных писем, в которых утверждается, что посылка не была доставлена или что возникла проблема
- **Фишинговая атака на юридическую фирму**: Сотрудники юридической фирмы не смогли распознать фишинговую атаку. Они получили электронное письмо, нажали на ссылку для загрузки документа, затем непреднамеренно ввели учётные данные для входа на то, что, по их мнению, было законным веб-сайтом, но привело к утечке данных.

B. Недавние фишинговые атаки, нацеленные бизнес в Великобритании.

Фишинговые атаки по-прежнему представляют серьёзную угрозу для бизнеса в Великобритании, и за последние годы произошло несколько заметных инцидентов.

- **Кибератака на библиотеку (январь 2024 г.)**: британская библиотека подверглась кибератаке, в результате которой её ИТ-системы вышли из строя. Группа вымогателей Rhysida взяла на себя ответственность за атаку и слила внутренние данные о персонале, включая сканы паспортов сотрудников и трудовых договоров, в даркнет
- **Мошенничество с предложениями работы в WhatsApp (ноябрь 2023 г.)**: Тысячи соискателей стали мишенью мошенников в WhatsApp, которые использовали поддельные предложения о работе, чтобы заманить жертв в свою схему
- **Фишинговые атаки на малый бизнес (2023)**: Исследование показало, что мошенничество и фишинг составляли 82% онлайн-угроз для малого бизнеса в Великобритании в 2023 году. Только в первой половине 2023 года число фишинговых атак по электронной почте выросло на 464% по сравнению с 2022 годом
- **Фишинговые атаки на организации Великобритании (2022–2023 гг.)**: 83% британских предприятий и благотворительных организаций, подвергшихся кибератаке идентифицировали фишинг как тип атаки

C. Недавние фишинговые атаки, нацеленные на частных лиц из Великобритании

Фишинговые атаки остаются серьёзной угрозой кибербезопасности в Великобритании, а различные недавние инциденты подчёркивают эволюцию тактики киберпреступников.

- **Фишинговая атака на Booking.com**: В ноябре 2023 года фишинговая атака была нацелена на Booking.com. Преступники осуществляли вишинговые (голосовой фишинг) атаки из колл-центров в Украине, выдавая себя за банковских служащих, чтобы оказать давление на жертв с целью перевода денег
- **Фишинговые атаки на парламентариев Великобритании**: В декабре 2023 года были совершены фишинговые атаки, направленные против парламентариев Великобритании из нескольких политических партий

- **Фишинговые атаки с мимикрией под правительственные электронные письма**: В 2022 году Национальный центр кибербезопасности (NCSC) сообщил о мошенничестве – фишинговые атаки проводились с применением поддельных писем, выглядящих как настоящие правительственные электронные письма

D. Фишинговые мошенничества, нацеленные на сотрудников

Фишинговые мошенничества, нацеленные на сотрудников, также известные как мошенничество с компрометацией деловой электронной почты (BEC), часто нацелены на руководителей или специалистов по персоналу, то есть должности, которые имеют доступ к конфиденциальной информации. Эти атаки обычно связаны с отправкой электронных писем, которые, как представляется, от старшего руководителя или CEO, с запросом банковского перевода или информации о заработной плате. К числу распространённых фишинговых мошенничеств, нацеленных на сотрудников, относятся:

- **Атаки на топ-представителей**: это целенаправленные попытки украсть конфиденциальную информацию у компании путём выдвижения себя за топ-менеджеров, таких как генеральные директора или CFOS
- **Фишинговые атаки с формой W-2**: в этом случае злоумышленник выдаёт себя за руководителя организации и отправляет сообщение сотруднику отдела заработной платы или отдела кадров с запросом W-2 информации
- **Фишинг новых сотрудников**: Новые сотрудники часто становятся мишенью, потому что они стремятся произвести впечатление и могут не замечать признаков фишинговой атаки

E. Фишинговые мошенничества, нацеленные на потребителей (обычных пользователей)

Фишинговые мошенники, нацеленные на потребителей, часто выдают себя за хорошо известные компании или организации, такие как банки или правительственные учреждения, чтобы завоевать доверие целевых лиц. Эти мошенничества обычно включают отправку электронных писем или текстовых сообщений, которые, как представляется, исходят от этих организаций, с просьбой предоставить потребителям личную идентификационную информацию. Затем мошенники используют эту информацию для открытия новых учётных записей на имя потребителя или вторжения в его существующие учётные записи. Некоторые распространённые фишинговые программы, ориентированные на потребителей, включают:

- **Мошенничество с обналичиванием чеков**: Мошенники нацелены на людей, продающих товары онлайн. Они переплачивают сумму с использованием расчёта чеком и просят перевести излишек обратно только для того, чтобы вернуть первоначальную сумму
- **Мошенничество с продажами**: Онлайн-покупатели, ищущие выгодную сделку, становятся мишенью для сайтов аукционов электроники высокого класса. Даже если потребитель не выиграет товар, ему все равно придётся заплатить
- **Мошенничество с трудоустройством**: предполагаемый работодатель проводит собеседование по телефону и сообщает соискателю, что он получил работу. Затем соискателя работы просят заполнить онлайн-кредитную форму, которая используется для кражи его личности

IV. УПРЕЖДАЮЩИЕ СТРАТЕГИИ

Фишинг является серьёзной угрозой кибербезопасности, и раннее обнаружение имеет решающее значение для предотвращения того, чтобы жертвы не стали жертвами этих атак.

- **Обнаружение фишинга на раннем этапе**: Раннее обнаружение фишинговых атак важно, так как 50% жертв становятся таковыми в течение 24 часов. Использование технологий и автоматизации может помочь выявлять фишинговые страницы раньше.
- **Использование DMARC**: DMARC – это глобальный стандарт аутентификации электронной почты, который помогает проверять происхождение электронных писем и блокировать поддельные из них. Это позволяет отправителям убедиться, что электронное письмо действительно исходит от того, от кого оно, по их утверждению, оно должно исходить
- **Мониторинг регистраций доменов**: Мониторинг регистраций доменов может помочь обнаружить мошеннические веб-сайты, созданные для кражи учётных данных, перенаправления веб-трафика или продажи контрафактной продукции. Такие сервисы, как PhishLabs и Red Points, предлагают услуги мониторинга доменов, которые могут автоматизировать процесс поиска и удаления поддельных учётных записей, приложений, веб-сайтов и доменов
- **Автоматизация обнаружения фишинга**: Машинное обучение может помочь обнаружить фишинговые атаки путём изучения шаблонов и создания моделей, которые могут автоматически отличать законные веб-сайты от вредоносных или другие формы коммуникации. Существуют также различные антифишинговые инструменты и сервисы, которые могут помочь компаниям защититься от атак
- **Сотрудничество между командами**: Сотрудничество между командами имеет важное значение для борьбы с фишингом. Регулярные тренинги по повышению осведомлённости персонала могут гарантировать, что сотрудники будут знать, как распознать фишинговое электронное письмо, даже по мере того, как методы мошенников становятся все более продвинутыми

A. Обнаружение фишинг на раннем этапе

Раннее обнаружение фишинга имеет решающее значение, поскольку жертвы наиболее уязвимы в первые 24 часа и для этого организации могут использовать различные технологии:

- **Автоматическое сканирование**: Использование инструменты автоматического сканирования для регулярного поиска фишинговых веб-сайтов и электронных писем. Эти инструменты могут сканировать и анализировать веб-страницы, электронные письма и другой цифровой контент на предмет признаков фишинга.
- **Машинное обучение**: Внедрение алгоритмов машинного обучения, которые могут извлекать уроки из моделей известных фишинговых атак и прогнозировать новые. Эти алгоритмы могут обрабатывать большие объёмы данных для выявления потенциальных угроз быстрее, чем люди.
- **Сообщения о пользователях**: поощрение пользователей сообщать о предполагаемых попытках фишинга. Быстрое создание отчётов может привести к более быстрому удалению фишинговых сайтов и предотвратить дальнейший ущерб.

B. Использование DMARC

DMARC используется как система проверки подлинности электронной почты, разработанная для защиты доменных имён от использования в фишинговых мошенничествах, подделке электронной почты и других киберпреступлениях:

- **Аутентификация электронной почты**: DMARC работает, гарантируя, что законная электронная почта должным образом аутентифицируется в соответствии с установленными стандартами DKIM (почта, идентифицируемая ключами домена) и SPF (структура политики отправителя).
- **Отчётность**: DMARC также предоставляет получателям электронной почты возможность сообщать отправителям о сообщениях, которые прошли или не прошли проверку.
- **Применение политики**: отправители могут устанавливать политики для того, как получатели должны обрабатывать почту, которая не проходит проверки подлинности, что потенциально предотвращает доставку мошеннических писем.

C. Мониторинг регистраций доменов

Мониторинг регистраций доменов может помочь выявить потенциальные фишинговые сайты до того, как они станут активными:

- **Службы наблюдения за доменами**: использование службы, которые отслеживают регистрацию доменных имён, похожих на бренд или товарные знаки.
- **Автоматические оповещения**: настройка автоматические оповещения для уведомления вашей службы безопасности о регистрации потенциально мошеннического домена.
- **Службы удаления**: использование служб, которые могут помочь удалить фишинговые сайты после их выявления.

D. Автоматизировать обнаружение фишинга

Автоматизация обнаружения фишинга предполагает использование программного обеспечения для выявления фишинговых угроз и реагирования на них:

- **Фишинговые базы данных**: использование базы данных известных фишинговых сайтов для блокирования доступа к ним.
- **Анализ в режиме реального времени**: внедрение системы, которые выполняют анализ веб-страниц и электронных писем в режиме реального времени для обнаружения фишингового контента.
- **Интеграция**: интеграция обнаружения фишинга в инфраструктуру безопасности, такую как брандмауэры, шлюзы электронной почты и endpoint решения, для комплексной защиты.

E. Совместная работа в разных командах

Сотрудничество является ключом к успешной стратегии борьбы с фишингом:

- **Межведомственное обучение**: проведение регулярных тренингов во всех подразделениях для ознакомления сотрудников с новейшими тактиками фишинга и способами их распознавания.
- **Обмен данными**: обмен данными о новых фишинговых угрозах между группами безопасности, ИТ-отделами и другими заинтересованными сторонами.
- **Планирование реагирования на инциденты**: разработка и применение на практике плана реагирования на инциденты с участием нескольких команд для обеспечения скоординированного реагирования на фишинговые атаки.

V. Программное обеспечение для обнаружения фишинга и реагирования на него

Программное обеспечение для обнаружения фишинга и реагирования на него представляет собой набор инструментов кибербезопасности, которые позволяют организациям выявлять фишинговые угрозы и устранять их. Несколько инструментов, которые можно использовать для автоматизации обнаружения фишинга:

- **Agari**: Этот сервис представляет собой систему реагирования на фишинговые инциденты, разработанную для ускорения сортировки фишинговых сообщений, судебной экспертизы, исправления и локализации взломов

- **IRONSCALES**: Эта самообучающаяся платформа безопасности электронной почты предназначена для активной борьбы с фишингом. Она сочетает в себе взаимодействие с человеком и идентификацию, ориентированную на искусственный интеллект, для предотвращения попыток фишинга, включая компрометацию деловой электронной почты (BEC)
- **Avanan**: Это антифишинговое программное обеспечение для электронной почты, размещённой в облаке, подключается к вашему почтовому провайдеру с помощью API для обучения его искусственного интеллекта на основе данных электронной почты. Служба анализирует не только содержимое сообщений, форматирование и информацию в заголовке, но и оценивает существующие отношения между отправителями и получателями, чтобы установить уровень доверия
- **Barracuda Sentinel**: Этот инструмент использует API почтового провайдера для защиты от фишинга, а также искусственный интеллект для изучения уникальных коммуникационных моделей вашей организации, чтобы выявлять и блокировать фишинг атаки и кибермошенничество в режиме реального времени
- **Proofpoint Targeted Attack Protection (TAP)**: Этот инструмент помогает организациям эффективно обнаруживать, смягчать и блокировать продвинутые целевые атаки, которые поступают по электронной почте
- **RSA FraudAction**: Этот инструмент специализируется на обнаружении и предотвращении попыток фишинга, троянов и мошеннических веб-сайтов
- **PhishER**: Эта облегчённая платформа управления безопасностью, автоматизации и реагирования (SOAR) помогает организовывать реагирование на угрозы и управлять большим объёмом фишинговых угроз
- **Zphisher**: Это инструмент для начинающих, который включает в себя несколько автоматических тестов на фишинг
- **Evilginx2**: Этот фишинговый инструмент описывает себя как платформу для атак типа "человек посередине", используемую для фишинга учётных данных для входа в систему вместе с сессионными файлами cookie, позволяющими обойти двухфакторную аутентификацию
- **DTonomy AIR Enterprise**: Этот инструмент на основе искусственного интеллекта включает в себя анализ фишинговых электронных писем в пакетном режиме, автоматизацию управления задачами и обращениями, а также сотни сборников игр

A. Основные функции программного обеспечения для обнаружения фишинга и реагирования на него

При выборе программного обеспечения для обнаружения фишинга и реагирования необходимо учитывать следующие ключевые особенности:

- **Идентификация домена**: возможность идентифицировать и проверять подлинность домена, с которого отправляется электронное письмо, помогая предотвратить подмену домена
- **Анализ Analysis**: анализ заголовков электронных писем на предмет несоответствий или признаков подделки, которые могут указывать на попытку фишинга
- **Анализ ссылок**: проверка ссылок в электронных письмах или веб-контенте, чтобы определить, ведут ли они на известные фишинговые сайты или вредоносный контент
- **Анализ атак имперсонизации**: обнаружение попытки выдать себя за законного юридического или физического лица. Это является типичным приёмом фишинг- атак
- **Аналитика искусственного интеллекта**: использование искусственного интеллекта для упреждающего выявления подозрительных моделей поведения и прогнозирования новых фишинговых угроз
- **Анализ с БД известных ссылок**: сравнение с базами данных известных угроз, которые часто обновляются вручную экспертами по безопасности, для выявления попыток фишинга
- **Отчётность для конечных пользователей**: позволяет пользователям сообщать о предполагаемых попытках фишинга, что может привести к более быстрому удалению сайтов мошенников и предотвращению дальнейшего ущерба

B. Как работают инструменты моделирования и тестирования фишинга

Инструменты моделирования и тестирования фишинга предназначены для того, чтобы предоставить пользователям реальный опыт борьбы с фишинговыми атаками:

- **Реалистичные симуляции**: распространение ряда реалистичных сценариев фишинга, имитирующих новейшие методы атак, включая вишинг (голосовой фишинг), для обучения пользователей
- **Регулярно обновляемые шаблоны**: использование шаблонов, которые часто обновляются, чтобы отражать новейшие тактики фишинга, гарантирует, что обучение остаётся актуальным
- **Частота автоматического тестирования**: автоматизирование частоты тестов на имитацию

фишинга обеспечивает последовательное обучение, а не спорадические, разовые сеансы

- **Тестирование в активной среде**: увидев фишинговое электронное письмо в активной среде, пользователи должны применить свои знания, чтобы не стать жертвой, усилив своё обучение
- **Идеи администратора**: с точки зрения администратора, внедрение симуляций и тренингов даёт представление об эффективности тренинга и состоянии безопасности организации

C. Внедрение программного обеспечения для обнаружения фишинга и реагирования на него

Эффективное внедрение программного обеспечения для обнаружения фишинга и реагирования на него требует сочетания технических решений, обучения пользователей и организационной политики. Связанные рекомендации:

- **Регулярное обучение сотрудников навыкам кибербезопасности**: Непрерывное обучение гарантирует, что сотрудники смогут распознавать попытки фишинга и реагировать на них.
- **Внедрение передовые методы обеспечения безопасности электронной почты**: использование протоколов, такие как DMARC, для проверки подлинности электронных писем и предотвращения подмены. Этот протокол основан на стандартах SPF и DKIM для проверки происхождения электронных писем и блокирования поддельных писем
- **Использование искусственный интеллект и автоматизацию**: ПО на базе ИИ может с высокой точностью сканировать входящие сообщения на наличие признаков фишинга. Алгоритмы машинного обучения также могут предсказывать новые фишинговые угрозы, изучая шаблоны известных атак
- **Отслеживание результатов фишинга**: использование инструментов моделирования фишинга для отслеживания реакции сотрудников на имитируемые атаки. Это может помочь выявить уязвимости и измерить эффективность обучающих программ
- **Фильтрация DNS-трафик**: Решения для фильтрации DNS могут предотвращать доступ пользователей к вредоносным веб-сайтам, блокируя запросы к доменам, внесённым в черный список. Некоторые фильтры могут предварительно проверять веб-сайты на наличие вредоносного кода и добавлять их в черный список
- **Использование технические решения**: применение надёжные пароли, DNS-фильтрацию, антивирусных решений, политик безопасного просмотра веб-страниц и использование службы безопасной электронной почты для предотвращения фишинговых компрометаций
- **Внедрение мер реагирования на инциденты и отчётности**: разработка плана реагирования на выявленную фишинговую активность. Это включает в себя шаги по исправлению положения и механизмы отчётности для устранения и смягчения последствий успешных атак
- **Использование шлюза безопасной электронной почты**: Развёртывание фильтров электронной почты, которые проверяют заголовки и вредоносный контент, классифицируют электронную почту и проверяют URL-адреса на соответствие репутации каналов
- **Защита пользовательских конечных точек**: Обеспечение безопасности пользовательских конечных точек путём внедрения средств защиты этих точек и обучения пользователей методам безопасного просмотра веб-страниц и электронной почты.

D. Ошибки реализации

При внедрении программного обеспечения для обнаружения фишинга и реагирования на него следует избегать нескольких распространённых ошибок:

- **Нерегулярное обновление программного обеспечения**: Регулярные обновления нужны, чтобы программное обеспечение могло эффективно обнаруживать новейшие фишинговые угрозы и реагировать на них
- **Чрезмерная зависимость от ИТ-отделов**: Хотя ИТ-отделы играют решающую роль в управлении и обслуживании программного обеспечения для обнаружения фишинга, важно, чтобы все сотрудники понимали, как выявлять попытки фишинга и реагировать на них
- **Вера в антивирусное программное обеспечение**: хотя антивирусное программное обеспечение может помочь обнаружить и предотвратить некоторые попытки фишинга, само по себе этого недостаточно. Решения для обнаружения и реагирования на конечные точки (EDR) и расширенного обнаружения и реагирования (XDR) могут обеспечить более комплексную защиту
- **Отсутствие продуманного моделирования фишинга**: Моделирование фишинга может быть полезным инструментом для обучения сотрудников распознавать попытки фишинга и реагировать на них. Однако важно проводить эти симуляции вдумчиво и чётко взаимодействовать со всеми соответствующими заинтересованными сторонами
- **Отсутствие продуманной стратегии защиты**: полагаться исключительно на антифишинговую программу может быть рискованно, поскольку злоумышленнику достаточно одной ошибки, чтобы добиться успеха. Стратегия комплексной

защиты, включающая несколько уровней безопасности, обеспечит более надёжную защиту

При выборе программного обеспечения для обнаружения фишинга и реагирования стоит опираться на следующие критерии:

- **Интеграция с другими инструментами**: Программное обеспечение должно быть способно интегрироваться с другими средствами обеспечения безопасности для комплексного подхода к безопасности
- **Возможности машинного обучения**: Многие современные инструменты используют машинное обучение для анализа действий конечных точек и сети и обнаружения потенциальных угроз
- **Определение приоритетности угроз**: ПО должно иметь возможность определять приоритетность предупреждений об угрозах, чтобы помочь вашей команде сосредоточиться на наиболее серьёзных угрозах в первую очередь
- **Агентный мониторинг против безагентного**: как агентный, так и безагентный мониторинг имеют свои плюсы и минусы, и может потребоваться их сочетание для оптимальной безопасности
- **Возможности мониторинга и анализа**: ПО должно быть способно отслеживать поведение конечной точки и обнаруживать, расставлять приоритеты, и оповещать о признаках компрометации (IoC) и признаках атаки (IOA)
- **Обнаружение против предотвращения**: Некоторые решения больше ориентированы на обнаружение попыток фишинга, в то время как другие – на предотвращение них
- **Автоматическое обнаружение угроз в режиме реального времени**: Эта функция может помочь вашей службе безопасности быстро выявлять угрозы и реагировать на них

VI. Риски фишинга в праздничные дни

A. Почему мошенники любят праздники

Мошенники любят сезон отпусков по нескольким причинам:

- **Повышенная онлайн-активность**: во время праздников люди более активны в Интернете, совершают покупки подарков, бронируют поездки и делают пожертвования благотворительным организациям. Эта возросшая активность предоставляет мошенникам больше возможностей обманом заставить людей раскрыть конфиденциальную информацию
- **Отвлекающий фактор**: Сезон отпусков – напряженное время, люди часто отвлекаются и могут быть не такими бдительными, как обычно. Мошенники пользуются этим, отправляя фишинговые электронные письма, которые, как представляется, исходят из авторитетных источников, таких как банки или популярные розничные продавцы
- **Эмоциональная манипуляция**: Мошенники часто используют эмоциональную манипуляцию во время сезона отпусков. Они могут выдавать себя за благотворительные организации или членов семьи, чтобы обманом вынудить людей отправлять деньги или раскрывать личную информацию
- **Сезонные темы**: Мошенники используют электронные письма, сообщения и веб-сайты праздничной тематики, чтобы обмануть жертв. Они могут отправлять поддельные электронные письма с заказами и отслеживанием, благотворительные электронные письма и сообщения, связанные с праздничными мероприятиями или расписаниями
- **Оппортунистическое поведение**: мошенники пользуются тем фактом, что многие компании предлагают бонусы или сезонные рабочие места во время праздников. Они создают фишинговые кампании, нацеленные на сотрудников с помощью поддельных предложений бонусов или на соискателей с помощью мошеннических объявлений о работе
- **Социальная инженерия**: мошенники используют тактику социальной инженерии, чтобы создать ощущение срочности или страха, например, заявляя, что посылка была пропущена или что учётная запись получателя была взломана. Это может побудить к поспешным действиям, таким как переход по вредоносным ссылкам
- **Поддельные интернет-магазины или “Магазины-двойники”**: мошенники создают мошеннические веб-сайты, имитирующие деятельность законных интернет-магазинов, чтобы обманом заставить потребителей вводить свою личную и финансовую информацию
- **Уведомление о пропущенной доставке / недоставке**: жертвы получают уведомления о том, что доставка была пропущена или посылка не была доставлена, с предложением перейти по ссылке, которая может привести на фишинговый сайт или установить вредоносное ПО
- **Мошенничество с подарочными картами**: мошенники рассылают поддельные электронные письма или текстовые сообщения с просьбой к жертвам приобрести несколько подарочных карт по личным или деловым причинам, часто выдавая себя за кого-то, кого знает жертва
- **Фальшивые благотворительные организации**: преступники создают фиктивные благотворительные организации и запрашивают пожертвования у людей, которые считают, что они вносят свой вклад в законное дело

- **Мошенничество в социальных сетях**: мошенники используют платформы социальных сетей для предложения праздничных акций, ваучеров или подарочных карт, требующих заполнения опросов, направленных на кражу личной информации
- **Мошеннические сезонные вакансии**: в Интернете размещаются поддельные объявления о вакансиях, предлагающие хорошие деньги за очень небольшую работу, ориентированные на людей, стремящихся подзаработать во время праздников
- **Фишинговые электронные письма**: они особенно распространены в сезон отпусков и могут принимать форму поддельных запросов на подтверждение доставки или других сообщений с целью получения личной информации
- **Кража данных**: Мошенники могут выдавать себя за службы доставки и отправлять мошеннические уведомления о краже посылки или проблемах с доставкой, чтобы обманом вынудить получателей предоставить личные данные
- **Мошенничество с отпуском**: предложения поддельных отпускных или туристических сделок, цель которых - украсть деньги или личную информацию у ничего не подозревающих жертв
- **Борьба с мошенничеством**: частным лицам отправляются нежелательные сообщения, которые могут показаться безобидными, но могут быть признаком того, что мошенник имеет доступ к личной информации получателя